House of Commons
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 023 • 1st SESSION • 39th PARLIAMENT

EVIDENCE

Monday, December 11, 2006

Chair

Mr. Tom Wappel

Standing Committee on Access to Information, Privacy and Ethics

Monday, December 11, 2006

● (1530)

[*English*]

The Chair (Mr. Tom Wappel (Scarborough Southwest, Lib.)): I'd like to call meeting number 23 to order. Pursuant to the order of reference of April 25, 2006, and section 29 of PIPEDA, we're continuing our review of part I.

We have a panel of witnesses today, and they are the Information Technology Association of Canada; Ian Kerr, the Canada Research Chair in Ethics, Law and Technology at the University of Ottawa; and the Canadian Bar Association.

I'll introduce the various people from the Information Technology Association of Canada: Bernard A. Courtois, president, and Ariane Siegel. Welcome. From the Canadian Bar Association we have Brian Bowman and Tamra Thomson.

Welcome to you all. We will let you all make a presentation....

Oui.

[*Translation*]

Mrs. Carole Lavallée (Saint-Bruno—Saint-Hubert, BQ): Mr. Chair, I apologize. I am so sorry, ladies and gentlemen.

As you know, we have before us a motion that we began debating at our last meeting. The purpose of this motion was to ask the Minister of Justice to introduce in committee, or in the House, no later than December 15—a date that is fast approaching; it's this Friday—strengthened and modernized access to information legislation.

It is extremely important that we discuss this motion, Mr. Chair, in order to remind the minister of his deadline and to ask him when he plans to come. He has only four days left. I would like to know when, during this meeting, we could discuss this motion, with all due respect to the witnesses we have formally invited here.

[*English*]

The Chair: Thank you, and thank you for the excellent synopsis of your motion.

The meeting was called for two purposes. First was to hear from the witnesses and second was to discuss committee business, namely, the report of the steering committee. If there is time after those two items, we can entertain your motion. If there isn't time, then that's the end of the meeting, which will end at 5:30.

I guess that's the answer to your question.

[*Translation*]

Mrs. Carole Lavallée: If there is not enough time left, could we postpone it to the next meeting; not tomorrow's meeting, since that is a special meeting, but to Wednesday's meeting?

[*English*]

The Chair: You can certainly advise us that you intend to proceed with that motion at that time on Wednesday. Is that your intent?

[*Translation*]

Mrs. Carole Lavallée: My intent was to talk about it today, Mr. Chair. Nonetheless, if we do run out of time, I just want to make sure that I will not have to re-table the motion with the clerk in order for us to discuss it on Wednesday.

[*English*]

The Chair: The clerk advises me that it's not necessary to retable since it is before the committee. We simply ran out of time when we discussed it last time. So is it your intention to raise the matter on Wednesday?

[*Translation*]

Mrs. Carole Lavallée: If we do not discuss it today, I intend to ask that we discuss it on Wednesday, or as soon as possible. It is a very urgent matter, Mr. Chair.

[*English*]

The Chair: That was not a trick question. Obviously if we have time today, we will go to it. Somehow I suspect that we won't, and that's why I asked you about Wednesday.

Thank you very much.

Tomorrow's meeting is a special meeting for one purpose only, Mr. Peterson.

These meetings are never boring for us. I'm sorry, witnesses.

Okay. As I was about to say, we'll hear from each of the groups. You each have up to ten minutes to make your presentation, and then we'll go directly to questions.

We'll start with the Information Technology Association of Canada and Mr. Courtois, please.

[*Translation*]

Mr. Bernard Courtois (President and Chief Executive Officer, Information Technology Association of Canada): Thank you, Mr. Chair.

Ms. Seigel will deliver our presentation, but I would like to say a few words first to put it into context.

Our association represents Canadian information and communications technologies, or the ICT industry, including everything to do with computers, software and telecommunications from equipment to service.

This industry is highly interested in every aspect of privacy protection, and has been for quite some time.

[*English*]

In 1996, when I was chief privacy officer at Bell Canada, we were already operating under an extensive set of regulations that dated back to 1955 in matters of privacy protection. But the industry as a whole, the broader industry, also saw at that time, as the Internet was about to explode in terms of usage, that privacy protection and confidence in the Internet and the e-economy was absolutely critical to our future. Therefore, our industry was really the first proponent of tackling the issue with legislation. We also had to consider that we couldn't take a regime that applied to a heavily regulated industry, like telecom was at the time, and transpose that holus-bolus to the whole economy in matters of privacy protection.

We were very happy to evolve a regime that was quite innovative and quite effective that involved a first layer of taking ten principles developed by the OECD in a multi-party manner, where they had consumers, businesses, and governments evolve these principles. They were taken, again, in a multi-party approach by the Canadian Standards Association, which developed a code on them. And the legislation reflects this, that we had a base of self-regulation on which we then imposed a government body, the Office of the Privacy Commissioner, in an ombudsperson role, and then the courts to do enforcement, if, as, and when required.

This mixed model, which, as I said, is quite innovative and quite effective, has been recognized worldwide as truly an effective way of tackling this, this made-in-Canada solution.

So I would say, when you hear suggestions, I would be very loathe to take on anything that changes the fundamental structure. There's really no reason to undo that very successful approach.

I have a final comment in terms of context.

● (1535)

[*Translation*]

The vast majority of the members of our association are small businesses and the vast majority of the businesses that are clients of our technology companies, who have to deal with these information protection measures, are small businesses. These businesses do not have the means to continually adapt to changes in their operating approaches.

[*English*]

They don't have in-house law departments; they don't have the resources to have a lot of legal advice to change the way they do things.

So I would say, again, as a general approach, our industry feels you should be very cognizant of the maxim that if it ain't really broke, don't fix it; don't change the legislation unless absolutely necessary.

I'll pass it on to Ariane.

Mrs. Ariane Siegel (Lawyer, Information Technology Association of Canada): Good afternoon.

My name is Ariane Siegel. I am a partner in the law firm of Gowling Lafleur Henderson, practising in the area of privacy and telecommunications law. I am also the chair of ITAC's privacy task force, and it is in this capacity that I'm addressing you today.

As you've already heard, a well-respected international think tank, Privacy International, ranked Canada at the top of the list of countries for privacy protection in its most recent survey—second only to Germany. The high degree of accessibility under PIPEDA did not go unnoticed by Privacy International, and the report correctly states that “anyone can complain to the Commissioner about an alleged violation of PIPEDA”.

ITAC suggests that contrary to the survey of 64 companies put before you by the Canadian Internet Policy and Public Interest Clinic, there has been a very good level of privacy compliance by Canadian organizations. Most organizations work diligently at compliance and have extended significant resources in this regard. Especially noteworthy is the profound impact that Canadian privacy laws are having on international privacy compliance. For example, many U.S. companies with Canadian subsidiaries are adapting Canadian privacy compliance frameworks for use in operational settings south of the border.

Let's begin with ITAC's general position regarding PIPEDA in the context of the ongoing review process. ITAC, as you've heard, believes it's far too soon to make significant changes to PIPEDA. Most companies have had less than three years to implement and refine their privacy policies and procedures. Furthermore, many customers and employees are only now becoming familiar with how to exercise their rights under the legislation. ITAC supports cooperation with industry to create guidelines for security implementation and operational standards to enhance the transparency and consistency of the exercise of existing powers under the legislation.

I'd like to focus on ITAC's views on several issues that have been raised over the course of this review process. First is with respect to PIPEDA's inherent flexibility. PIPEDA's flexibility allows for the implementation of privacy principles in all organizations, no matter how large or small, and across all industries, however different their business processes may be. Consumers and employees also benefit from PIPEDA's flexibility, which provides an accessible, effective, and low-cost dispute resolution mechanism.

Secondly, with respect to the commissioner's order-making powers, ITAC believes that the existing ombudsperson model provides an effective, informal, accessible, and cost-effective dispute resolution process, while also allowing for a formal and binding review process by the court in certain instances. If decisions of the commissioner were to become binding orders, organizations would have to implement a more formal and costly compliance infrastructure. Adherence to PIPEDA's broad principles would give way to a very strict and literal approach and much less openness and collaboration with the Office of the Privacy Commissioner. Binding orders also raise the stakes for businesses in any dispute, and consumers could expect to find themselves pitted against experienced legal counsel in the process. Such a formal and adversarial process might well be avoided by consumers altogether.

Next, with respect to mandatory data breach notification, ITAC opposes mandatory notification of privacy breaches. ITAC is of the view that organizations take their responsibilities for data security very seriously. In the case of a data breach that poses risk to individual privacy, no organization would want to take on the additional potential liability of not taking adequate steps to mitigate further risks or damages that could be suffered to individuals. Many organizations currently contact the Office of the Privacy Commissioner to get guidance on how to deal with data breaches.

ITAC is of the view that mandatory notification requirements would result in notification fatigue for customers. CIPPIC pointed out in its submissions to this committee that several U.S. jurisdictions currently have notification requirements in place. However, these notification requirements do not mean that privacy protection is better in the United States or that somehow Americans are less prone to identity theft.

● (1540)

Canada is an international leader on the data protection front. Canadians have also been early adapters of leading-edge technologies, and many of the organizations are in the forefront of leading efforts to develop new privacy-enhancing technologies and processes. ITAC would support and would itself be interested in working with the Office of the Privacy Commissioner to develop guidelines on addressing data breaches.

[*Translation*]

Another issue is the commissioner's discretion to identify complaint respondents.

Currently, case summaries are reported for the most part on an anonymous basis. The commissioner has taken the position that naming respondents in each and every case would not meet the public interest threshold of the legislation.

ITAC supports this approach. The commissioner has the discretion she requires in order to name respondents. ITAC believes that a mandatory practice of naming respondents in each and every instance would not benefit parties to any dispute, and, in fact, could result in negative consequences.

Complaint resolution often results in a change to business policies or procedures such that the benefit naturally accrues to all customers. In this way, positive results are achieved with a high degree of efficiency.

[*English*]

Fifth, ITAC would like to respond to the issue of increased restrictions on transborder flows of personal information. Commercial practices often demand that personal information flow across borders. This has become an irreversible economic reality, driven by globalization and new technological opportunities.

Fortunately, PIPEDA's accountability principle demands that businesses in Canada communicate their privacy practices to the public and requires businesses to enter into contractual agreements to ensure a similar level of protection for personal information transferred outside of Canada.

Placing further restrictions on transborder flows of information under PIPEDA could reduce the global competitiveness of Canadian businesses. Canadian privacy legislation does not need to be modified to ensure that organizations safeguard data in any outsourcing, whether local or transborder.

PIPEDA very clearly recognizes the need for organizations to safeguard data. The Office of the Privacy Commissioner has set out a very practical framework for dealing with transborder data outsourcing in two recent case summaries.

Most importantly, the long-established common law of agency imposes obligations on organizations to protect data in their custody and control and would extend to the need to impose adequate protection when data is processed elsewhere.

In conclusion, ITAC believes that the provisions of PIPEDA are sound and continue to provide the appropriate balance between the interests of the public and industry as technology and expectations evolve over time. PIPEDA balances various legislative approaches, setting the tone for other jurisdictions and enabling Canadian businesses to remain competitive in the global arena.

ITAC members have invested significantly in the operational, legal, technical, and training aspects of privacy protection. ITAC itself has demonstrated leadership in educating its members about privacy, and we have worked with the federal and provincial privacy commissioners in doing so. We plan to continue our efforts in this field.

On behalf of ITAC and its member companies, I would like to thank you for the opportunity to address this committee.

● (1545)

The Chair: Thank you very much.

We'll now go to Professor Kerr.

Mr. Ian Kerr (Canada Research Chair in Ethics, Law and Technology, University of Ottawa, As an Individual): Good afternoon, Mr. Chair and honourable members.

Let me commence by expressing my extreme gratitude for the invitation and the opportunity to appear before you today on a set of issues that I care very deeply about.

Like many of the others who have appeared before you, and perhaps unlike my friends to my left, I'm concerned that there are a number of significant problems with the current legislation that do require reform. I've provided written submissions to that effect and hope to illustrate a key problem in my brief time before you here today.

The Chair: Go ahead.

Mr. Ian Kerr: I submitted them about a week ago. They perhaps didn't come through translation.

It perhaps goes without saying that computers, databases, networks, surveillance cameras, cookies, spyware, radio frequency identification, and other automated means of collecting, using, and disclosing personal information directly threaten our ability to control personal information.

You've heard about this from many of your previous witnesses. I have significant expertise on these issues, and I'm happy to provide more information about any of them for you, if you wish, during the question period.

My testimony today, however, will be to suggest that there is a much bigger threat to privacy that comes from a much more primitive and much more basic technology. It is a technology that all of you are familiar with, even those of you, like our honourable chair, who avoid computers, PDAs, and the Internet like the plague.

The threat I'm referring to is in fact a legal threat.

[*Translation*]

In French it is called the “contrat d'adhésion”.

[*English*]

In English, we call it the standard form contract.

While computers, surveillance cameras, and RFID chips technologically enable aggressive, voluminous, and sometimes surreptitious collection of information, it is the standard form contract that legally enables the so-called “implied consent”, “deemed consent”, and “opt-out” consent-gathering processes that are said to justify the use of surveillance technologies under our current privacy law. These means of using the law to deem consent, when there is in fact none, can be highly problematic.

Standard form contracts are mass-produced documents that prevent and preclude negotiation and agreement. They are drafted exclusively by parties in an economic position to offer them on a take it or leave it basis. In an information age, where the business handshake has been replaced by mouse clicks, where the bilateral negotiation process is supplanted by global, one to many transactions, the standard form contract is regularly invoked by organizations to circumvent various privacy protections prescribed by PIPEDA and other data protection regimes.

Whether in the sale of goods or the licensing of services, many organizations use standard form contracts, clickwraps, and end-user licence agreements as ways to justify what is sometimes an unreasonable and overarching so-called consent to excessive collection, use, and disclosure of personal information. Through these sometimes one-sided contracts, organizations are able to extend their personal information practices well beyond the bounds of what might otherwise be permitted by Canadian privacy law. They do this by compelling consumers, customers, and citizens to sometimes contract out protections that would otherwise be afforded through PIPEDA.

In my written submissions, which I guess you don't have in front of you, I offer a series of detailed recommendations on how to amend PIPEDA in light of these, to fix the enormous problems of obtaining genuine consent that are generated by the contractual model.

I am happy to answer any questions you might have on those, but let me first provide you with two crunchy examples that should hit close to home.

Example number one. As a member of Parliament, your job, like mine, requires you to stay in one of Canada's nearly 400,000 hotel rooms from time to time. Maybe you need to send some documents or check your e-mail while you are there. To use a hotel's Internet services, you'll be required to agree to its terms of use. On a recent work-related trip, I stayed at a Hilton Hotel. While there, I needed to use the Internet. Here is what I'm said to have consented to when I plugged my computer into the Hilton's Internet connection:

> We automatically track, collect and compile User Information and Transaction Data (as defined below) when you utilize the Site.
>
> ...
>
> You agree that HHC shall own all Information.
>
> By accessing the Site, you voluntarily, expressly and knowingly acknowledge and agree with all of the foregoing and further agree to each and all of the following: (i) such Information belongs to HHC and is not personal or private proprietary information; (ii) such Information, wherever collected, may be processed, used, reproduced, modified, adapted, translated, used to create derivative works, shared, published and distributed by HHC in its sole and absolute discretion in any media and manner irrevocably in perpetuity in any location throughout the universe without royalty or payment of any kind, without, however, any obligation by HHC to do so;
>
> ....

So instead of me, let's imagine that the honourable member, Mr. Tilson, stayed at the Hilton Hotel and sent an e-mail to his colleague, Mr. Wallace, an e-mail containing some communications perhaps about these committee deliberations, perhaps about some more personal things.

Under the terms of service referred to above, Hilton will claim that the personal information and private communications generated by these two honourable members is in fact not personal or private information, by way of their consent, and it is therefore not subject to PIPEDA, and that in fact Hilton owns the information in perpetuity, anywhere in the universe. As David Bowie might have once sung, “Planet Earth is blue, and there's nothing you can do”.

According to Canadian contract law—and I've been teaching it for more than ten years—I suspect that Hilton would likely prevail. Regardless, most individuals would be forced into submission during a lengthy and protracted litigation process in the courts about what is certainly, at this point, an unclear point in the law. I recommend we clarify the law with this.

Example number two. Like me, everyone around this table is a consumer of many intellectual products every day. You read the newspaper, specialty magazines or books, or maybe you watch TV, movies, or listen to music or talk radio. If you are like me, sometimes you don't care who knows what you are reading about or listening to, and sometimes you probably do, but l'II bet that you would care a lot if you learned that someone was always able to know about every single intellectual product that you consumed: how often, where, when, etc. Everyone around this table, I suspect, cares about intellectual privacy, the ability to consume intellectual products free from public scrutiny and corporate or governmental surveillance.

● (1550)

Imagine that you go out and buy a CD or DVD, or maybe you borrow it from the library. You put it into a device that you own and you play it. You watch or you listen. All the while, unknown to you, a small software routine written into the code of that CD or DVD causes an automated communication via your wireless Internet connection. The CD or DVD reports back to Sony—or whoever—who you are, where you are, what machine you use, which software you run, what you are watching or listening to, when you watched or listened, how often, etc.

By now in the course of these proceedings, and having heard many witnesses, you are, I suppose, no longer surprised by the realities of the digital age, but here is something that might surprise you.

You decide to investigate whether the company's practice infringes on your privacy rights under Canadian law. You come to learn that it probably does not, or at best that the law is unclear with respect to any of this. In fact, you come to learn that you have probably legally consented to letting the CD phone home and rat you out to the mother ship. ln the standard form contract of more than 3,000 words—which, by the way, is about 700 words more than it took Edgar Allen Poe to tell the tale of the thousand injuries of Fortunato—52 words provide your so-called consent to the automatic installation of a rootkit; Sony calls it “a small proprietary software program”.

Because of this provision, the organization collecting your personal information will claim that you have contracted out of the protections otherwise afforded to you under PIPEDA. According to their agreement, you also supposedly consented to allow them and their information-sharing partners to give that information to any member of the government who makes a request, without a court order and without any form of due process—and there is nothing you can do about it.

The main point I want to impress upon this committee today is that this form of legal manoeuvring—something that each and every one of us around this table is subject to multiple times each and every day—is hugely problematic and is not sufficiently addressed in PIPEDA. Standard form contracts, as well as a number of other so-called consent-gathering processes, can sometimes—not always, but sometimes—undermine the nature and value of genuine consent, and in those instances will fly in the face of what our privacy laws are actually trying to achieve.

I would submit that PIPEDA's attempt to balance individual privacy rights with the needs of organizations to collect personal information is undermined if—irrespective of PIPEDA's many protective provisions—intrusive, unfair, or unwanted collection, use, or disclosure can be imposed on individuals with impunity through standard form contracts or other similar so-called consent-gathering processes such as those used in the past by Sony, by Hilton and other hotels, by instant messaging services, by mobile phone providers, by other online service providers, by health care providers, etc. I can assure you this same strategy is used often and with great success in other sectors as well, all of which tells us we do need much tighter sets of consent provisions than those currently provided in PIPEDA.

ln my written submission, I offer concrete recommendations to fix this. If I have another thirty seconds, I'll go on the record to lend my support for other recommendations that have been made by other witnesses. In particular, the law should be amended to provide the federal Privacy Commissioner with order-making power; the law should remove any lingering doubt about the power of the federal Privacy Commissioner to regularly name names in well-founded findings; the law should include a mandatory security breach disclosure requirement; and finally, Ottawa must seriously begin to address the growing concern in Canada over the outsourcing of personal information to non-Canadian organizations, particularly data flows to the United States.

I know there is no time to address these points now, but I am happy to respond to any questions you might have.

Thank you very much for your time.

● (1555)

The Chair: Thank you very much, Professor.

Yes, we did receive your material. It's in translation, and it will be distributed to everybody.

We definitely thank you for your concrete recommendations, and we'll take a look at them. I, for one, thought that Hilton's standard foreign contract was very nicely worded. It must have been drafted by Gowling or McCarthy.

Some hon. members: Oh, oh!

The Chair: We'll now go to the Canadian Bar Association and Mr. Bowman.

Ms. Tamra Thomson (Director, Legislation and Law Reform, Canadian Bar Association): Mr. Chair, I will start and then Mr. Bowman will continue.

The Canadian Bar Association is very pleased to appear before this committee as it conducts its statutory review of PIPEDA. The Canadian Bar Association is a national association representing over 37,000 jurists across Canada, and amongst our primary objectives are improvement of the law and improvement of the administration of justice, and it's with those optics that we have reviewed PIPEDA, and indeed that we were actively involved when PIPEDA was developed.

The development of this area of law also led the Canadian Bar Association to establish the privacy and access law section, the group that has prepared the paper before you. I'll just say something about the section. It brings together lawyers who act for businesses and not-for-profit organizations and privacy groups, as well as academics, and government officials who act in this area of law. So it brings that balance of interests to the table in assessing the operations of the law.

Finally, a word about the paper in front of you. This is not the privacy and access law section's first foray into a review of PIPEDA; we've provided preliminary assessments to Industry Canada and the Privacy Commissioner on issues that we thought should be addressed in this review. So the paper before you poses some key points from those more comprehensive submissions and gives an executive summary of them. We have provided the full paper to the clerk for use in greater detail.

I will now ask Mr. Bowman, who is chair of the privacy and access law section, to address the key elements that we think are subjects to review.

● (1600)

Mr. Brian Bowman (Chair, National Privacy and Access Law Section, Canadian Bar Association): Mr. Chairman, honourable members, thanks very much for the opportunity to speak with you today.

In my brief remarks to you this afternoon, the CBA section wishes to highlight four key areas or themes among several we've addressed in detail in our submission to Industry Canada, which we've just referenced.

These themes reflect particular areas of PIPEDA that six years of experience have demonstrated to be deficiencies in the law or that represent emerging policy issues that were not adequately recognized when the law was first enacted. After nearly six years of interpretation by the courts and by the Office of the Privacy Commissioner, we believe it's prudent and necessary to consider amending PIPEDA.

Privacy legislation has been enacted in British Columbia, Alberta, and Ontario since PIPEDA came into force. These provincial developments respond to our experience with PIPEDA and in some instances have addressed deficiencies in both drafting and interpretation.

The CBA section's recommendations for amendments to PIPEDA are shaped by the following principles. First, while respecting the balancing of interests in the collection, use, and disclosure of personal information, vigilance is necessary in monitoring and opposing unnecessary erosions of privacy by both government and non-governmental organizations. Second, the basis for protecting privacy in Canada should be fair information practices as they continue to evolve. Third, privacy legislation and practices across Canada should be harmonized to the extent possible.

I'll touch on the first theme, and that is that PIPEDA should be neutral in regard to the litigation process. In other words, it should not affect pre-existing and commonly held litigation processes that have evolved for decades and hundreds of years. PIPEDA contains a number of specific exemptions to the consent requirement that require amendment. The current exceptions relating to litigation are too narrow and should, at a minimum, be broadened to ensure that well-established litigation procedures are not impeded.

This narrowness is evident in the investigation exceptions, the one-way disclosure, the collection and use of debt disclosure information, and the limitation on disclosure throughout the litigation process. The result is inadequate coverage of all aspects of the process: pleadings, oral discovery, mediation, private arbitration, settlements, solicitor communications, and other non-court ordered exchanges of information.

There should be a broad exclusion for information legally available to a party to a proceeding that would override specific exceptions currently found in PIPEDA. Related to this concern, PIPEDA should be amended in its application to law enforcement. Specifically, the provisions for the collection, use, and disclosure of personal information without consent for legitimate law enforcement purposes should be clarified. The current provisions relating to investigations and the enforcement of laws are confusing and internally inconsistent. A single standard should be applied for collection, use, and disclosure relating to law enforcement.

Finally, the provisions respecting investigative bodies should be streamlined. For example, organizations should be permitted to carry out their own investigative activities without unnecessarily being required to use other investigative bodies to collect information from third parties. The CBA recommends an amendment to create a broad exclusion for information available by law to a party in a proceeding to permit collection, use, and disclosure without consent where reasonably required for an investigation.

The second theme I'll touch on is as follows: PIPEDA enforcement should be more effective while continuing to reflect principles of fundamental justice. The lack of order-making powers in PIPEDA significantly affects the likelihood of complainants bringing forward issues of non-compliance. Complainants must apply to the Federal Court to obtain a remedy or compensation, but they may only do so after the commissioner has issued a finding. At present, it takes up to a year to receive a finding. Also, taking a matter to the Federal Court effectively requires hiring legal counsel and places the complainant at risk of an adverse cost award.

Further, there is no mechanism for the commissioner to compensate an individual who has incurred significant expense or suffered loss in connection with a complaint. However, under the current structure, conferring order-making powers on the commissioner could result in a violation of principles of fundamental justice. Currently, the commissioner acts as an ombudsman who advocates protecting personal information. The commissioner's office also investigates alleged violations of PIPEDA. Combining advocacy, investigative, and decision-making roles may place the commissioner in a conflict of interest and undermine the credibility of the office.

● (1605)

More effective enforcement could be achieved by assigning a separate office or body, functioning in a reasonably informal manner with decision-making authority. We've previously suggested an impartial tribunal with order-making powers and the ability to award damages, while the commissioner would retain the investigative powers and an advocacy role. The commissioner could be required to issue a finding within six months, which would then be referred to the tribunal. Therefore, the CBA section recommends an effective enforcement mechanism for PIPEDA be considered, such as an establishment of an impartial tribunal that would operate relatively informally, with power to make orders and award damages.

The next theme is that any requirement for notification of breaches of privacy should be balanced in approach. To date, federal and provincial privacy legislation has required public and private organizations to apply security safeguards when handling personal information. Several U.S. states have recently enacted additional legislation to require organizations to notify individuals in the event of a security breach involving improper disclosure of their personal information.

The EU has recently announced that it may consider information security incident notification. In contrast, Canadian privacy legislation does not explicitly contain such a requirement, with the exception of Ontario's Personal Health Information Protection Act. Therefore, the CBA section recommends that a balanced privacy breach notification requirement be considered, such as a duty to notify only where an organization is not covered by security mechanisms such as encryption, or has received notice that such protection mechanisms have been breached, and the information that has been compromised is sensitive personal information.

The final theme I'll touch on is that transborder information intended under Canadian privacy laws to flow unimpeded should be subject to appropriate precautionary requirements.

The commissioner has stated that the review of PIPEDA would be an opportunity for developing further privacy protection measures related to transborder information sharing by the private sector. One such measure is found in the commissioner's submission to the British Columbia Privacy Commissioner concerning the impact of the U.S. Patriot Act on personal health information of B.C. residents. The federal Privacy Commissioner recommended that Canadian companies that outsource information processing to organizations based abroad should notify their customers that the information may be available to the foreign government or its agencies under a lawful order made in that country.

Section 17 of Quebec's Act Respecting the Protection of Personal Information in the Private Sector specifically addresses the issue of transborder transfer of information. It obliges people communicating information about Quebec residents to persons outside the province to take all reasonable care to ensure that such information is not disclosed to third parties without consent, except as provided in the legislation.

PIPEDA currently contains general rules requiring parties holding information or outsourcing information to ensure its protection, but doesn't necessarily contain any rule specifically directed at protection of information transferred outside of Canada. Under PIPEDA, each organization, as you know, remains responsible for personal information in its custody or control, including information transferred across a border.

PIPEDA should contain appropriate precautionary requirements to protect information when it is transferred across borders. We have previously considered a number of alternatives to achieve this objective, such as a requirement that organizations transferring information to foreign entities enter into written agreements that would ensure security and protection of information against unauthorized access or disclosure in accordance with Canadian privacy law. Another alternative is a more generalized approach of protecting information transferred outside of the jurisdiction found in Quebec's privacy law.

In its earlier submission, the CBA section also analyzed options for notification or consent requirement for information transferred across a border. Each of these options would involve some form of notice to be provided to or consent obtained from the individuals whose information would be transferred outside of Canada. Amending PIPEDA to implement either a notice or a consent requirement to cross-border transfer of information requires a very careful consideration of the potential advantages and disadvantages of the approach.

The CBA section recommends that where personal information is to be stored or processed in a jurisdiction outside of Canada, PIPEDA require additional provisions to enhance security of personal information and ensure conformity to Canadian law, such as contracts between organizations and entities storing or processing personal information.

● (1610)

The CBA section appreciates the opportunity to share its views with the committee today. We believe our suggestions will provide some assistance in amending PIPEDA to address deficiencies that have become apparent since its enactment. Our goal is to improve the legislation for the benefit of Canadians, consistent with PIPEDA's purpose of establishing rules that recognize both individual privacy rights and the organizations' needs to collect and use information in an appropriate and reasonable manner.

Thank you very much.

The Chair: Thank you.

We will begin round one, with seven minutes per questioner. Right now, I have Mr. Dhaliwal, Madame Lavallée, and then Mr. Tilson.

Mr. Dhaliwal.

Mr. Sukh Dhaliwal (Newton—North Delta, Lib.): Thank you, Mr. Chair.

Is there a point of order?

Mr. Mike Wallace (Burlington, CPC): No, I just want my name on the list.

Mr. Sukh Dhaliwal: I thought you were going to need a point of order for the next two hours.

I'm just kidding, Mike.

Thanks, witnesses, for coming and giving us your presentation.

Professor Kerr, it was quite scary to hear the way you presented that any information or anything we do on the computer, basically, irrespective of whether it's at the Hilton Hotel lobby, at home, or at our business, is not protected under the privacy laws.

Mr. Ian Kerr: Actually, I would clarify. I picked some particularly dramatic examples that I thought would grab hold of this audience. I would never suggest that every standard form contract is written in these kinds of ways. In fact, many good counsel, both at the table and around the room, have worked hard to try to have balanced provisions in these kinds of things.

The main point I wanted to make, however, is that the threshold for consent in contract law is very low. Contractual consent is a transactional notion. It occurs in a moment. It occurs when I click "I agree"—and you know as well as I do that most people around the room, when they're forced, with those standard form agreements, go scroll, scroll, scroll, click, click, click. Even in cases where you try to read them, sometimes they're very difficult.

So in answer to your question, it's not the case that every good or service online would be such as to circumvent PIPEDA, but the point is that they can and the point is that the consent provisions within PIPEDA have to be clarified in such a way that this low threshold of clicking for consent and other kinds of deemings of consent don't have the effect of undermining the privacy protections that are meant to be there notwithstanding people's contracts.

Mr. Sukh Dhaliwal: Ms. Siegel, you presented that PIPEDA is working at this point in time. Are you aware of any privacy breaches that might have occurred in the last three or four years since it came into effect?

Mrs. Ariane Siegel: Am I aware of any privacy breaches?

Mr. Sukh Dhaliwal: That's right.

Mrs. Ariane Siegel: Certainly I come across issues with respect to privacy breaches often. The question is, are these breaches serious, and what do companies do about them? In fact, every organization that I've ever dealt with has always approached the Privacy Commissioner for guidance on what to do with their privacy breach.

In many cases, the privacy breaches are so insignificant—for example, an e-mail address. I'd say 99.9% of any of the privacy breaches I've encountered are accidental releases of someone's e-mail address. It's as simple as—and I'm sure everyone at this table has experienced it—sending that in the header of an e-mail and exposing the other people you're sending the e-mail to. That might be considered by some to be a privacy breach, and that's the reality of many of the privacy breaches.

With respect to consent issues and are consent issues and privacy breaches somehow tied together, PIPEDA goes into great, great detail with respect to what is a reasonable form of consent. The schedule to PIPEDA provides all sorts of examples with respect to what's a reasonable form of consent. Certainly it has become commonplace, in my experience. Every single company that I've ever dealt with puts together different standards of consent, based on the sensitivity of the information.

Organizations that are collecting sensitive personal information, such as financial data, almost always exclusively use express forms of consent; whereas if consent is just for purposes of secondary marketing, sending you literature in the mail about the organization or about maybe a sale going on down the street that you might be interested in...most individuals are very happy with implied forms of consent, and that's working quite well under PIPEDA. The Privacy Commissioner herself has recognized this in a whole string of decisions going back a few years now.

Really, the issue of consent is almost a settled piece of guidance within PIPEDA. Virtually no organization or no individual really gets too riled up about consent these days.

● (1615)

Mr. Sukh Dhaliwal: Mr. Bowman said that certain amendments can be made to PIPEDA.

What is your view? Are you satisfied that it's fully working? Is there anything you see that can be modified?

Mrs. Ariane Siegel: I think it depends on the perspective you're coming from.

With respect to transborder data flow, ITAC members don't believe that amendments are necessary under PIPEDA. The Privacy Commissioner, in two recent decisions—and you're probably familiar with them already—has carefully articulated guidelines with respect to what you need to do in the case of a transborder data flow. All companies now routinely use non-disclosure agreements and contracts.

If you look back in history at why organizations use contracts when they enter into any outsourcing arrangement, whether it's local or transborder, it's because the common law of agency and principle requires you to do that. You don't really need legislation to put that into practice; the law has already done that for you.

Mr. Bernard Courtois: If I may add something, when I talked earlier about being careful not to amend the law if it's not really necessary, as I heard from the Canadian Bar Association, there's one category of information for investigations pertaining to litigation. We have no views on that. That might well be required. I know if you change the law there, you're not going to change people's day-to-day lives such that they're now going to have to interpret things differently. It's going to be law firms doing interpretations.

On the lack of order-making power, I think creating a separate tribunal would really be adding another heavy layer. It would create another government institution with our taxpayer dollars and another place complainants would have to go to. I'd be very leery about that.

On the question of cross-border data flow, British Columbia tried to legislate that. It caused an awful mess. They were going to grind the health care system to a halt. They tried to make significant amendments to address it. The Privacy Commissioner has issued decisions that give very clear guidelines as to how you have to treat that. And it's the same with consent. The appendix talks about "knowledge and consent" in 4.3.2, meaningful consent, and in 4.3.5, "reasonable expectations of the individual".

I think we're not talking about having to change the law; we're talking about how you interpret the law reasonably in a given circumstance.

The Chair: Thank you, Mr. Dhaliwal.

We'll now go to Madame Lavallée.

[*Translation*]

Mrs. Carole Lavallée: Thank you very much, Mr. Chair.

My first question is for the representatives from the Canadian Bar Association. Is there a law other than the Privacy Act that similarly protects the identity of the respondents, those who break the law? Is there another law like that?

[*English*]

Mr. Brian Bowman: Just so I'm clear on the question, are you asking if there is another law that protects non-complying organizations or individuals?

[*Translation*]

Mrs. Carole Lavallée: No. I am talking about identity.

The Privacy Act protects the identity of the respondents, in other words, the names of the companies violating the law. Is there, in Canada or in certain provinces, other laws that also protect the identity of the respondents?

M. Bernard Courtois: I can try to give you an answer, Mrs. Lavalée.

The law we are talking about does not prevent the disclosure of identity. The commissioner decides on a case-by-case basis whether this is reasonable or not.

● (1620)

Mrs. Carole Lavallée: You are right to make this clarification.

I want to know whether there are other laws that protect the name of the infringing companies in this way.

[*English*]

Mr. Brian Bowman: In your question, do you mean that do not permit the various commissioners in the provinces to disclose the identity of infringing organizations? I'm not aware of any provincial statutes that prohibit the respective Privacy Commissioner from disclosing the identity of an infringing organization.

[*Translation*]

Mrs. Carole Lavallée: I did not think I was asking such a complicated question. I will re-word it.

Under the law, the commissioner can, or cannot, disclose the identity of the respondents. The fact remains that identity is not automatically disclosed. For example, if I am arrested for impaired driving, my name will surely appear in the media somewhere. However, no one decides whether my identity should be disclosed or not.

I would like to know whether there are other laws under which the identity of the respondents is not automatically made public. Is that a better way of phrasing my question?

[*English*]

Mr. Brian Bowman: Off the top of my head, I'm not actually aware of any.

[*Translation*]

Mrs. Carole Lavallée: Thank you very much. That was a good answer. There was no wrong answer. In fact, I wanted to know what you thought. This helps me a great deal, despite what you might think.

Spokespeople from the Department of Industry appeared before the committee as witnesses and they informed us that the Privacy Act was the object of a constitutional dispute in the Quebec Court of Appeal.

Are you aware of this initiative and these issues? Could you comment on that?

[*English*]

Mr. Brian Bowman: No, I'm afraid I'm not in a position to speak about those issues. Like other lawyers, I'm waiting to see how the challenge unfolds. In terms of the issues that are at play, I certainly wouldn't be in a position. Nor has our section put its mind to analyzing that for the purposes of the PIPEDA review.

The Chair: Professor Kerr, do you have any comments on that issue?

Mr. Ian Kerr: I would also disclaim any particular expertise on the issue. The issue, of course, is a constitutional issue, so it has to do in part with the fact that PIPEDA, as you've heard from other witnesses who've appeared before you, tries to achieve ends that can be understood as falling within both federal jurisdiction as well as provincial jurisdiction.

I actually don't have any particular comments that I think would enlighten this committee. Therefore, I'd rather not obfuscate by making my opinions known.

The Chair: How about ITAC?

Mr. Bernard Courtois: It's not an issue that we have addressed as an association, so we have no expertise to bring.

[*Translation*]

Mrs. Carole Lavallée: I have another question for the representatives from the Canadian Bar Association and perhaps for anyone else who wants to comment.

The privacy commissioner has talked about the difficulties she has encountered when, during investigations, she has wanted to access documents that were protected by solicitor-client privilege. She said this hindered her ability to investigate.

Do you have an opinion on this?

[*English*]

Mr. Brian Bowman: We certainly heard her remarks to this committee, but specifically addressing that issue, again, we haven't put our minds to it. What I can do is perhaps redirect this to the recommendations that we've put forward in terms of the overall functioning of the office right now. But directly on that point, I apologize again that we haven't put our minds directly to it.

Mr. Ian Kerr: I'd be happy to comment on that.

I was here on the day when Madame Commissioner was making her submissions to this committee. I would, quite frankly, be quite surprised if somehow solicitor–client privilege operated differently for the commissioner in terms of her investigations than it would for other investigatory bodies. From what was going on that day, I was quite unclear exactly on what it was that was being sought. If there is solicitor–client privilege, and if that privilege is such as to preclude other investigatory bodies from getting that evidence, it's not clear to me why the Privacy Commissioner should have that over and above other investigatory bodies.

● (1625)

[*Translation*]

Mrs. Carole Lavallée: Mr. Courtois.

M. Bernard Courtois: We haven't addressed this issue either. Mr. Kerr's comments seem reasonable, but that is no reason to add special powers in the legislation. I have nothing more to add.

Mrs. Carole Lavallée: Frankly, I haven't been lucky, Mr. Chair.

[*English*]

The Chair: Actually, you got answers.

[*Translation*]

Mrs. Carole Lavallée: The answers are interesting.

Do I have any time left?

[*English*]

The Chair: No.

[*Translation*]

Mrs. Carole Lavallée: Thank you.

[*English*]

The Chair: Mr. Tilson.

Mr. David Tilson (Dufferin—Caledon, CPC): Thank you.

You know, you're the first ones who have raised this issue. The solicitor–client privilege issue hasn't really been raised since the commissioner was here. Most of you, if not all of you, are lawyers. I always thought that lawyers would get terribly excited on that topic. Solicitor–client privilege is a big deal, and she's recommending that it change.

Ms. Siegel, what do you think?

Mrs. Ariane Siegel: I can't imagine why the treatment of documents in an investigation would be different for the Privacy Commissioner than in the context of any other examination or ombudsperson model, especially given the context of her role. It's my understanding the commissioner approves and enjoys the role of ombudsperson and is not seeking order-making powers.

I know of no situation where documents that are covered by solicitor-client privilege should in fact somehow become part of the commissioner's investigation process.

Mr. David Tilson: I'm not going to go any further. I expect you're all going to agree on that.

On the question, however, of order-making powers, today it's two to one against you, Ms. Siegel. I don't know what the overall count is, but that's an interesting issue. I don't know what the overall count is, but certainly it's an issue that needs to be debated by the committee.

I want to go on a little further. The difficulty is, of course.... The commissioner has said—as someone has just pointed out—it's on a case-by-case basis, and it was Mr. Bowman who raised the issue that there is no way to compensate loss. I think it was Mr. Bowman who said that.

There is the other issue of violations: violations of lack of consent, violations of lack of notification, violations of any breach of the legislation. That's if you find out it's happened. I can't believe there aren't going to be all kinds of examples where we don't even know. For instance, the passing around of lists all over the place. Someone told us that the commissioner has rarely imposed this rule of notifying the public that there have been violations.

I know you've all commented on this, but it's very important, because if you're going to have any teeth to this legislation—and I'm really directing my questions to you, Ms. Siegel, because you're the one who said the ombudsman process should continue. Will the legislation have any teeth without order-making powers?

Mrs. Ariane Siegel: I can only turn to experience, to the experiences of my members and my own experiences advising businesses on compliance.

First of all, I think we need to separate order-making powers from a duty to notify. First, with respect to order-making powers, order-making powers are not what will enhance privacy protection in our society. I don't think the Privacy Commissioner is looking for order-making powers. And setting up a type of tribunal for the Privacy Commissioner would have to seriously alter how we view the role of the Office of the Privacy Commissioner right now. It would change from that of an ombudsperson and an advocate-educator to that really of a tribunal, which is significantly different.

Order-making powers, I don't believe, are something you would want to see for privacy issues. For any of you who are familiar with the privacy dispute process, I've had the opportunity to be involved in a number of mediations with the Privacy Commissioner, and when you're involved in this sort of mediation and a dispute or a complaint against you, companies put on the table all of their most complex business processes.

The issue is, should somehow a tribunal be struck to deal with and order new processes for business? My suggestion is that's not something you would want to see happen. There are very few bodies, or individuals even, who have that sort of detailed business process expertise that goes to the root of some of the issues we're discussing today.

● (1630)

Mr. David Tilson: Mr. Bowman commented on compensating loss. Are Mr. Bowman's clients going to have to rely on tort law or contract law? Is that what you're saying?

Mrs. Ariane Siegel: But that's the case for all other claimants in society who feel they've somehow been wronged or suffered a loss.

When we're dealing with privacy breaches, in some instances they may result in some form of loss, but in the vast majority of instances they may not. And when it's appropriate and they have suffered damages, then it's open to them, as it is open to any other claimant in a society, to go to Federal Court and seek damages. I don't think we necessarily need to have in place a completely different system to treat losses in the privacy context.

The commissioner herself, I believe, sees that she's had ample ability in fact to help mould and change the direction of how companies comply with privacy. So, for example, if you've gone to the Privacy—

Mr. David Tilson: Mr. Bowman wants to join in on this, so maybe you could wind up.

Mrs. Ariane Siegel: When you go to the Privacy Commissioner's website, for example, you'll see the whole host of findings that she has listed, and in very few instances has she had any trouble whatsoever in convincing an organization that it should somehow change its process. I'd say one of the most important instruments in her back pocket is the threat and the possibility that if an organization does not change its practices, she can use her power to name names.

Mr. David Tilson: I bet she's only done it a couple of times.

Mr. Bowman.

Mr. Brian Bowman: Thank you.

One thing we should say for the record is that the CBA, we think, has a balanced approach on a lot of these issues. On this issue, I think it actually is quite evident. In my statements, I wanted to reinforce the fact that our recommendation for order-making power is conditional upon an impartial tribunal model. We don't necessarily think the status quo is perfect, nor do we think that just slapping down order-making power for the Privacy Commissioner is the answer.

Mr. David Tilson: Somewhere out west—I don't know which one it is, Alberta or British Columbia—they have non-appealable decision-making power. What would you think of that model?

Mr. Brian Bowman: We looked at both the Alberta and British Columbia models in coming up with our recommendations, but despite that and input of members from those jurisdictions, the recommendation was really to try to create a model in which the strengths of the Privacy Commissioner's Office advocacy investigations are left as they are, and to set up this tribunal with order-making powers. The reality right now is that companies that handle personal information simply don't fear the consequences of being found acting contrary to PIPEDA. I would agree that the naming of names is a stick. I wouldn't say it's a big stick, and I think that's reflected in our submission. This is coming from organizations and firms such as my own who advise private companies.

The Chair: Mr. Tilson, you're way over time, but I see Ian's hand up, so I'll recognize him.

● (1635)

Mr. Ian Kerr: The professor doesn't put his hand up that often.

Some hon. members: Oh, oh!

Mr. Ian Kerr: I think in the context of the conversation we were just having, it's useful to note that of the more than 1,400 complaints that the Privacy Commissioner has received, only nine cases, as far as I can count them, have been commented on by the Federal Court, and not a single one has attracted a damage award, as far as I can tell. Three of the complainants were able to recoup their costs; four of the cases saw the court awarding no costs to either party; in two cases the complainant had to bear the costs for themselves as well as for their opponents. I would suggest that part of the impetus behind PIPEDA was a recognition that the private law was insufficient as a means of remedying some of the potential problems in an information age.

So I would suggest that the question isn't whether without order-making powers this legislation has any teeth. The question is, what kind of teeth make for the best system? If you would like me to continue, I would say why I think order-making power is important, but I'll leave it to the chair.

The Chair: I'll let someone else ask that question, because we're over time.

Just so we can be clear on this solicitor-client privilege issue, I want to quote directly from the commissioner's testimony before us. By the way, has anybody on the panel actually had an opportunity to literally read the decision in Blood Tribe? No.

She says this:

> It [the decision] effectively allows organizations to shield information from our investigators with no independent verification that the documents in question do in fact contain information subject to solicitor-client privilege.

That's what she said. The way I read that, it seems to be that she's afraid someone could say, "Oh, you can't have that because it's subject to solicitor-client privilege", and there's no way of checking to determine whether or not that alleged solicitor-client privilege is in fact in law. Would any of you have any problem, assuming that's the decision, if there were an independent way of verifying whether or not a solicitor-client privilege claim was in fact accurate?

I see a shaking of heads in the negative. Are we all agreed that it would be reasonable to at least have someone determine whether the claim was verified?

Some hon. members: Agreed.

The Chair: Okay. Thank you.

We now go on to the second round, which is for five minutes each. We have Mr. Peterson, Mr. Wallace, Mr. Van Kesteren, and Mr. Stanton at the present time. Should anyone else want to, just put up your hands.

Hon. Jim Peterson (Willowdale, Lib.): Following up on Mr. Tilson's questioning about order-making power, one of the complaints I imagine is, is it going to Federal Court? It's very costly and time-consuming. It's an intimidating thing for an individual to have to do.

Having said that, what about looking at a tribunal that could...? You'd give the commissioner order-making power and then you would allow a tribunal to decide, and it would be more of an informal tribunal, as the Canadian Bar Association has suggested.

Mr. Courtois.

Mr. Bernard Courtois: I would feel uneasy about that. I think the brunt of what people see going on and the statistics quoted by Professor Kerr show there really isn't a problem. I would hesitate to say we're going to legislate another regulatory body just because we think we might be able to improve things.

This isn't broken, and it does not require more regulation and another regulatory tribunal.

Mr. Ian Kerr: I would like to go on the record as saying there's more than one way to interpret what those statistics say with respect to whether there is a problem or not. That should be obvious to the members, but I want to go on the record as saying that.

Mr. Brian Bowman: Part of our submission, and the reason for suggesting the tribunal, was based on what we see as a potential conflict between the competing responsibilities of the commissioner's office. When you think about it, the commissioner's office is responsible for educating, for investigating, for helping mediate, but also for acting essentially as the judge. So that conflict and our recognition of that is reflected in our suggestion for this tribunal.

Hon. Jim Peterson: People would have to have a lawyer if they're going to a tribunal, wouldn't they?

Mr. Brian Bowman: I don't think so. I'm not looking for new work.

● (1640)

Hon. Jim Peterson: I'm thinking of my friend Paul here.

Mr. Brian Bowman: Our suggestion is an informal tribunal, so it is just that; you wouldn't have to go to court. Currently, you have to go to court and you have to wait up to a year to get a recommendation from the commissioner's office. So I don't think the current framework is helping those—

Hon. Jim Peterson: Taking the Federal Court out of it and having this less awesome tribunal—no appeals to the Federal Court—was Mr. Tilson's question.

Mr. Brian Bowman: That's not our recommendation. Ultimately, the Federal Court could weigh in.

Hon. Jim Peterson: So for a "deep pockets" organization you'd go to mediation, then you'd go to the tribunal, and then you'd go to the Federal Court?

You've all dealt with three different provincial laws and you've also dealt with the federal. What did you learn in terms of what the best law is in looking at all four jurisdictions? Are the suggestions for change based on one of these systems being better than the others? And where's the lack of harmonization?

The Chair: Which one of you would like to respond?

Hon. Jim Peterson: The bar mentioned the lack of harmonization, so let me start with that one. Then the next one would be what are your recommendations flowing from these?

Mr. Brian Bowman: Sure. The short answer is that there was a preference for some of the provincial acts, notably Alberta and British Columbia.

I'm flipping to my business transaction section, and that is a good example of where the provincial laws have learned from the PIPEDA experience. The drafters learned from the deficiencies and the lack of clarity in PIPEDA, specifically dealing with due diligence investigations in the sale of a business and a recognition that lack of clarity in PIPEDA is not assisting business. It's not assisting with the protection of privacy or the facilitation of—

Hon. Jim Peterson: These are the areas where you want better definitions, as in the appendix?

Mr. Brian Bowman: Yes, and with the business transactions, without referencing them, the B.C. and the Alberta legislation in particular set out expressly what organizations are to do to protect privacy.

For instance, if you're going to sell your business and you want a prospective purchaser to take a look at your personal information holding, right now it is unclear when and how they can view that, if at all, under PIPEDA. The Alberta privacy legislation spells it out. And for organizations that don't have deep pockets, that makes it a lot more business-friendly, so they don't have to retain people like me.

The Chair: Thank you, Mr. Peterson.

Mr. Wallace.

Mr. Mike Wallace: Thank you, Mr. Chairman.

Thank you for the presentations tonight.

I have a few questions. We've heard a lot about this organization and this legislation in the last few weeks.

Following up on Mr. Peterson's question, and it was one of my questions for the Information Technology Association of Canada, you indicated that you think the present system on order-making powers is fine. Since you are a Canadian organization, and I believe there are order-making powers in British Columbia, for example, have your members had an issue with that? Would you like to expand on that a little bit?

Mr. Bernard Courtois: I would say we have no indication that where there's an order-making power, there's better implementation of privacy protection. In other words, the ombudsman process is simpler and more straightforward for both complainants and the companies involved, and it seems to be producing good results. I've not had anything that says the B.C. situation produces better privacy protection—maybe a little more work for lawyers, I suppose. The way we get feedback, not just from the statistics but from our members, is that once you get an investigation by the Privacy Commissioner, all the pressures are there for you to change your behaviour.

Mr. Mike Wallace: Just so I have a better understanding, who are your members?

Mr. Bernard Courtois: About 70% of our members are small companies and 30% are larger companies, 70% Canadian-based. It's a very international industry, maybe about 30% multinationals—not the same overlap, because there are some Canadian-based multinationals. They're involved in computers, all kinds of computer technology, mobile technology, telecommunications technology, software, information technology services, and consulting. There are a lot of very small software companies, a lot of small companies. Canada, for example, is a world leader in security software and that kind of—

● (1645)

Mr. Mike Wallace: Has there been an increase in cost due to the introduction of PIPEDA?

Mr. Bernard Courtois: Yes, at first, in the sense of trying to adapt to a new law, to create processes in the firm to respond to it. But they do not begrudge that, because as I said, this is an industry whose very livelihood is dependent on good privacy protection. Except that once you go through a whole process of education—and as I said, there are two layers. There's self-regulation, where the businesses themselves have to learn about this, get educated, and comply. That's where I get a little leery about changes to the law that would require them to study everything again.

After a few years, we're still in the process of getting all this to filter through and getting people comfortable with what they have to do. And technology changes so much that they have to keep up to speed on that as well. So they've got plenty on their plate with that already.

Mr. Mike Wallace: Professor Kerr, I have just a couple of questions for you.

I want to be clear, because we don't have your presentation in front of us. Your standard form issue really deals with consent. That's an accurate statement?

Mr. Ian Kerr: Absolutely.

Mr. Mike Wallace: When we get it, your presentation will deal with those issues in written form? Is that accurate? Is there anything we don't have in front of us that you wanted to tell us briefly about the consent issue and standard form? I think I understood it, but....

Mr. Ian Kerr: Sure. I'm more than happy to provide my oral remarks. What I had already provided was a written submission, which was much more formal in nature, but I'm happy to provide this as well.

Mr. Mike Wallace: There are recommendations in the formal piece, right?

Mr. Ian Kerr: There are several recommendations.

Mr. Mike Wallace: Okay. Let's use your Hilton example. I'm not sure they're reading our e-mail or they know I use it at 10 o'clock at night. I'm sending it across the world, and they might need a different service provider as a Hilton organization. But when is it my responsibility? There's a consent form I'm supposed to read and I submit yes or no. Is that not my responsibility, to read that thing?

Mr. Ian Kerr: It's absolutely 100% your responsibility to read it, and Canadian contract law is very clear in this regard, that so long as sufficient notice has been given.... In cases such as Rudder and Microsoft, which is one of the leading cases in Canada...it is incumbent upon the person who ultimately clicks “I agree” to either read those terms or to be deemed to consent if they don't. However, the point is it's not just about reading, knowing, and understanding them; it's about the idea that in an information age, where there's only one choice, which is either yes or you don't get to participate, it raises issues with respect to the relative bargaining power of the individual. I would suspect that many times in your life you have been faced with that situation where you have no—

Mr. Mike Wallace: But it's a choice. Isn't it the glory of living in this country that we have a choice we can make? Either I get on the Internet and talk to my friend David that night or I decide I wait because I'm not satisfied that it's secure enough. When does the government get out of the way of individuals making that choice?

Mr. Ian Kerr: I would suspect—

The Chair: Thank you.

Professor, that's just a rhetorical question. We don't have to get into a debate on it.

Mr. Mike Wallace: I thought it was a good question.

Mr. Ian Kerr: It's a very important question, and I'd like to answer it if you let me.

The Chair: All right. I'll let you both...and I see another hand up.

Mr. Ian Kerr: In the context of when those kinds of things are such that courts and governments ought to interfere with those contracts, that's your question, under what circumstances ought they too. In my recommendations I'm very clear that where the privacy legislation itself has an elevated standard of protection such that, for example, in the British Columbia statute it says you're not allowed to prevent somebody from withdrawing from their consent at a later time, and if you attempt to do that the contract will be unenforceable.... The B.C. legislation, for example, says that. What I'm recommending to you here is the same sort of thing. So just like in the law of contracts the courts will set aside contracts as being unenforceable for public policy or illegality when somebody tries to contract something that goes against a statute, I'm suggesting the same with PIPEDA. In other words, when a PIPEDA protection is there, you shouldn't be exposed to having somebody ram down your throat that you're not allowed to avail yourself of those protections or else not use any services. That's my submission.

● (1650)

The Chair: And in reply, Ms. Siegel.

Mrs. Ariane Siegel: First of all, the law in this area is actually quite well developed. The law, as Professor Kerr is aware, requires companies not only to provide information in their terms of use, for example, and to get individuals to click "I agree", but you're also required to highlight any important part of those terms and conditions to your customers. Many of you have probably seen these in terms of use; you'll have a bold statement going across the page that says, look out below, there's something important, and you'll point it out.

Secondly, in the case of a collection of personal information like the example that was provided, which is too broad, PIPEDA provides the perfect mechanism to be able to redress that. PIPEDA clearly says you can only and should only collect personal information to the extent that it's required and use it to the extent that the use is reasonable. There are a whole series of Privacy Commissioner decisions that look at this very issue. And when an organization is collecting excessive amounts of information or using it in an inappropriate way that is too broad, there is a redress mechanism that is provided, and the commissioner is able to find findings and recommendations against the respondent. From my experience, companies are absolutely terrified of the Privacy Commissioner. All you have to do is hold up the example of the Air Canada case so many years ago and they say, "We don't want that to be us; that's the last thing we want." That's the most important tool the commissioner has.

If you look at the American jurisdictions that do have notification requirements, and I believe at the last count there were 22 U.S. jurisdictions, privacy protections are no better there. It's the opposite. In fact, how many of you have seen those notification letters that come in the mail? You can get a dozen of them in a week sometimes in some jurisdictions, and they become meaningless. All it does is infuriate many consumers, who say, "My gosh, is this serious or not? What am I supposed to do?" Much preferable would be a mechanism whereby industry and the Privacy Commissioner come together to have guidelines with respect to how you deal with notification and data breaches. I'm sure most organizations would happily follow along.

The Chair: Thank you.

I for one think the Hilton contract dealing with the universe is entirely too broad. I think it should be limited to the planet earth.

Monsieur Plamondon, s'il vous plaît.

[*Translation*]

Mr. Louis Plamondon (Bas-Richelieu—Nicolet—Bécancour): My question will be brief because I have to leave at 5 p.m.

Mr. Kerr, could you clarify something for me? When you talked about the commissioner's powers, the interpreter used the term "order". I thought I understood she could issue orders. At least, that's what we got in the French translation.

Did you talk about orders? If yes, could you give some clarification on the recommendation you gave on this?

[*English*]

Mr. Ian Kerr: No, I did not.

[*Translation*]

M. Bernard Courtois: I think the intention was to talk about order-making powers, like a court has.

Mr. Louis Plamondon: Then the interpreter did not provide the right word.

Could you clarify this anyway?

[*English*]

Mr. Ian Kerr: One of the things I said right in the closing part of my remarks, as a recommendation, was with respect to order-making power, which we've talked a bit about so far today. I did not in any way suggest that the commissioner currently has that power.

[*Translation*]

Mr. Louis Plamondon: When the commissioner testified before the committee, she did not seem very much in favour of the idea of having such power. She wasn't looking for it. I was therefore surprised by the contradiction in terms of a certain obligation we would have given the commissioner.

[*English*]

Mr. Ian Kerr: I would like to comment on that, if you'd let me. I came to hear the commissioner speak, and I also heard Commissioner Loukidelis from British Columbia speak. I've also been sort of following what's been going on online with people who are discussing these proceedings on blogs.

I would love to put forward my take on this, because I think I heard it differently from how some people have been talking about it subsequently. What I heard the commissioner say was that at the moment she is not in favour of order-making powers, and she was very clear that she was open to the idea of potentially wanting them. Further, she said that this is not the right time for her to have order-making powers. She also alluded to some things that some people might have interpreted as having to do with some of the transitions, which have taken place in that office, over the past several years.

I also heard Commissioner Loukidelis describe the order-making power as a power of last resort, which I believe some people around this table misunderstood as him somehow denigrating as an unnecessary power. I think a power of last resort is an extremely important power. When a tightrope walker walks on the tightrope and the safety net is the instrument of last resort, just because it's the last resort doesn't mean it's any less important. In fact, it's potentially the most important instrument.

So I would be careful to draw conclusions from the fact that when she was a commissioner in Quebec, she had order-making power and because she is now the Privacy Commissioner of Canada and has suggested that this is not the time for order-making power, that this means order-making power is inappropriate.

As a manager, she recognizes that the office has been through a tremendous amount of turmoil in the last several years, and she takes the position, like my colleagues over here, that maybe it's too soon for these powers. I want to be very clear that it's not at all the case that she has in any way suggested that she is against the idea of order-making power.

● (1655)

[*Translation*]

Mr. Louis Plamondon: Thank you, Mr. Chair.

Mrs. Carole Lavallée: Do we have any time left?

Mr. Louis Plamondon: If there is any time left, I would like to give it to my colleague.

The Chair: Yes, you have a minute left.

Mrs. Carole Lavallée: Thank you, Mr. Plamondon.

I would like to come back to the debate that was well underway on the matter of consumer consent. I do not know whether this was described as abusive, but that is the adjective that comes to mind. We were talking about the consent that Hilton Hotels asks for and all the consent we are asked for. We sign consent forms with the idea that the consent seekers cannot do much with it anyway. But often, the information ends up on the Web.

Furthermore, consumers are not very familiar with the Privacy Act. They are not very aware of their rights either. This is perhaps one reason why there are not very many complaints.

The fact that publishing the identity of the respondents is left to the discretion of the commissioner does not help us either in better understanding the law. Often, we learn about our rights by reading the newspapers and hearing about individual cases that do not comply with the law. I am also re-reading the US Patriot Act, which suggests that consumers be advised when their personal information goes abroad. I do not see how consumer protection fits in this system. How can a consumer refuse to give his consent?

I am not sure whether you each want a turn to comment, if that is alright with Mr. Chair, of course.

[*English*]

The Chair: Fifteen seconds each.

Mr. Ian Kerr: Obviously, from my previous remarks, it's clear that I share some of your concerns with respect to the consumer protection aspect of this. Quite frankly, I'm surprised that the recommendation I was putting forward is somehow thought to be extraordinary in any way. With this recommendation, I'm not asking for a major overhaul of anything to do with PIPEDA. I'm simply suggesting that where a contract comes into conflict with other higher order privacy protections under the act, we should clarify the act to say those contracts are unenforceable.

I agree with my colleague that with respect to the reasonableness clause, it may operate in that way to do this. In theory, it should operate to do that. You're going to find situations where, when consumers are confronted with that, the party on the other side will simply say, "Well, look at our contract. How can you say that anything around our information-collecting practices are unreasonable under PIPEDA if you've already agreed to them by way of contract?"

You make my point for me in a way.

The Chair: And the CBA?

Mr. Brian Bowman: Our position is that the current consent model doesn't need revision. The illustration that was pointed out in terms of being able to read the contract and make a decision is a reasonable approach.

That being said, the reality is that the Hiltons of the world are getting away with some of these consent provisions that might be too broad. That's why we focused our energies on the enforcement mechanisms, in terms of order-making power being contingent upon a tribunal set-up.

● (1700)

The Chair: Thank you.

[*Translation*]

Mr. Bernard Courtois: The current law does not allow abusive behaviour. It is therefore not necessary to amend it to allow—

Mrs. Carole Lavallée: In your opinion, is the Hilton Hotel's behaviour abusive?

Mr. Bernard Courtois: In my opinion, if someone complained to the commissioner, you would see a rather quick change in the company's behaviour. I do not see the need for order-making power to make a company like that comply. I think this would happen quickly enough.

[*English*]

The Chair: Thank you.

I would remind committee members what the commissioner said, and I quote:

> We will not be asking for enhanced enforcement powers. We are not convinced that the time is right to make such a fundamental change to the enforcement mechanisms for several reasons, both practical and administrative.

She expanded on that during questions.

Mr. Van Kesteren.

Mr. Dave Van Kesteren (Chatham-Kent—Essex, CPC): Thank you, Mr. Chair.

Thank you all for coming out.

I have a question for Ms. Siegel or Mr. Courtois. What's the thinking behind what Professor Kerr has brought forward, the contracts we don't sign but we click onto...? Why do hotels and organizations like—

Mrs. Ariane Siegel: Hotels—and I think it's unfair to pick on the Hilton hotels—in general have to balance their interest in protecting consumer information. The Hilton, or any other hotel, probably has no real interest in owning the personal information or exercising that sort of power. They have to balance, though, the language they use in their contracts against the practical realities of protecting their own interest.

What happens, for example, if you have a guest who is using the hotel's resources, the computer, to access illicit or illegal websites and is perhaps engaging in illegal transactions? They have to have the recourse to go to that individual and say they looked at this and it's not right. Whether it's legal or not, they have to balance a whole variety of interests, not only the interests in Canada but also the interests internationally. There may be requirements in the United States with which they are complying or requirements in Europe they have to consider.

My experience is that many organizations are trying their best to put together terms of use and privacy policies. They have to balance a whole variety of obligations and compliance issues, and privacy is only one of them. Maybe someone hasn't looked that carefully at the privacy language. But I bet if you asked Hilton, or other organizations that have similar policies, whether they really intend to use personal information for those purposes, I'm sure the answer would be no. Really, their only interest is in protecting themselves and making sure they are able to comply with the variety of obligations they have in front of them.

Mr. Dave Van Kesteren: Professor Kerr, rather than reinvent the wheel, when it comes to e-mail and such, couldn't you enact a law that extends privacy to those things? Then the things that Ms. Siegel is speaking of really wouldn't be an issue. We can all understand what she is talking about; it's the e-mail. That's the stuff that scares everybody. Could that be done?

Mr. Ian Kerr: I suppose it could be done. It would go against what most people who appeared before this committee have said, including the Privacy Commissioner of British Columbia. He made some significant remarks about this principle called “technological neutrality”, which to some extent is a principle I subscribe to as well.

I don't necessarily think there is something magical about e-mail that means we need a special law. I think the recommendation I put forward is in the spirit of what you're suggesting. It simply says that in situations where somebody is seeking consent through a standard form agreement for the purposes of things that are excessive and unreasonable, PIPEDA would clearly state that those contracts are unenforceable.

● (1705)

Mr. Dave Van Kesteren: I have another question, and this one is to you, too, Professor.

You were talking about the iPod and its capability, and being able to track people and find out exactly what they're listening to. Who cares? Who really cares if I'm listening to Alabama? Oh, shocking!

Mr. Ian Kerr: I would suggest that question provokes what I think is the fundamental misunderstanding by the general public about data protection...and falls short of understanding its importance, the whole reason we're doing this.

The former commissioner—I'm talking about Bruce Phillips—described PIPEDA as a necessary step in addressing some of the erosion of privacy that comes with computers and networking, and ultimately to reverse that.

If you understood the extent to which information collected for one purpose can be amalgamated with other information for secondary purposes, and if you understood the kinds of colleagues I work with and the kind of information they can glean by data mining and putting information together, you would see that eventually what we're talking about here is the idea that it could be possible, with these systems, that every kind of intellectual product you consume could be databased and therefore a narrative could be put together by connecting the dots.

It's really not about your listening to Alabama one night. It's a profile of your life. It's the sort of thing that scared the bejabbers out of Justice Bork in the United States in terms of video movie rentals. There was a subpoena, when he was being nominated for the Supreme Court, to find out what videos he was collecting. Now imagine that with every single thing you read, look at, listen to, watch, or think about. All of the intellectual products, by virtue of being in the digital realm, are to some extent capable of that level of observation.

Mr. Dave Van Kesteren: Do I have a little more time?

The Chair: No, you're at six minutes already, I'm afraid. We can come back to you on another round, though.

Mr. Peterson.

Hon. Jim Peterson: On notification of breach, do you think there should be an obligation to consult with the commissioner if you're not going to notify?

The Chair: Is that addressed to all?

Hon. Jim Peterson: To Ms. Siegel. Sorry.

Mrs. Ariane Siegel: That's an issue that would have to be taken up with our members. But certainly many organizations with which I'm familiar now do consult often with the Privacy Commissioner's office, and I don't think they would see a different duty.

Mr. Bernard Courtois: We've got a law already that allows the commissioner to determine when it would be reasonable to notify and when it would not. So why would we need to legislate something that, by nature, is going to have to be more rigid than reasonableness would require?

Hon. Jim Peterson: Is there any counter to that?

Mr. Brian Bowman: Some of the challenges with duty to notify have been addressed by some of the other guests here in terms of notification fatigue. Our detailed submission sets out our views on notification of loss. We say if a duty to notify is to be directly or indirectly included in PIPEDA, it should be a balanced approach.

Bill 200 is a bill I assisted with drafting in Manitoba. It's intended to be substantially similar to PIPEDA, modelled after the Alberta law. It has a duty to notify. It reflects the similar language we've put in our submission in terms of a balanced approach. For example, we say that a duty to notify might be included where the information is about an identifiable individual or the information is not identifiable by virtue of being protected through, for instance, encryption, or the organization has received notice that the protection has been breached, that the encryption technology has been breached, and that the information falls into certain specified categories of sensitive information.

If you say duty to notify every time, you're going to end up with notification fatigue. It's going to be ineffective. The status quo and the reality are that some organizations simply choose not to notify, and that may not be friendly from a privacy perspective.

● (1710)

Mr. Ian Kerr: I don't have anything to add.

Hon. Jim Peterson: Mr. Kerr, you said the commission experienced considerable turmoil in previous years. Would you like to elaborate?

Mr. Ian Kerr: Not particularly. The media has done a fairly good job of speaking about some of the hardships that occurred in that office with the previous commissioner. I don't need to add anything.

Hon. Jim Peterson: Thank you.

The Chair: Thank you, Mr. Peterson.

Mr. Tilson.

Mr. David Tilson: I'd like to talk about an area, and it's a form question I ask all witnesses, and that has to do with small business. In my riding, people know there was a scandal somewhere in the past with one of the privacy commissioners and they're worried about identity theft and all that entails, but people who talk to me don't even know about this. And of course the Privacy Commissioner has given testimony at this committee that much of what she does is about educating the public, and I expect PIPEDA would concur with that.

I've had people in my riding, small business people, people who work out of their homes—I mentioned at the last session a dry cleaner, or it could be a small retail person, a small business person—haven't a clue about all this stuff; they really don't. The commissioner can go all over the country giving speeches and sending out literature.

I'm addressing this question to all three groups. Do you have any recommendations as to what we could do with the legislation to assist the small business person?

We can start off with Ms. Siegel.

Mrs. Ariane Siegel: I don't think changing the legislation in any way is going to help small business. What will help small business, number one, is investment in resources with respect to education; number two, practical guidelines that businesses across the board can implement; number three, working groups that establish precedents and model agreements that can be implemented by small businesses; and number four, new technologies and investment in new technologies, which can be used by small businesses and all businesses in helping to safeguard data.

These practical tools will help businesses and in turn help consumers the most.

Mr. Bernard Courtois: An accumulation of studies coming out in the last few months shows that the Canadian economy is made up of predominantly small business, and small business in Canada needs help in getting to know more about how to use technology. So to the extent that we can do things that encourage that or encourage them even in the tax system to invest more in technology...we will help the system, but at the moment we have a big gap in the use of technology by Canadian small business.

Mr. Ian Kerr: I agree with absolutely everything that's been said so far, and some of my recommendations about tightening up the consent provisions are made because at the end of the day small businesses are going to have to have a clearer sense of how to do that. That can also be helped, to some extent, through guidelines and through educational systems.

I know the Privacy Commissioner's office is already committed to those kinds of educational campaigns. They've been ramping up a lot of their online modules, some of which I know because my colleagues and I have been involved in facilitating the development of some of those kinds of tools. The Privacy Commissioner's office also started a landmark kind of thing that I've not seen in any other jurisdictions that care about privacy. It's a contributions program meant to have academic involvement from across the country in developing the very kinds of tools you're talking about.

It's still early days in terms of that. And in the same sense that you've heard from some of the witnesses appearing before you that it's early days and small business hasn't yet crystallized how to do this, so don't change the rules, I think the same is true for thinking about the educational mandate. It's rolling out now, and I would encourage more and more of it. But it's only fair to say that this Privacy Commissioner has been deeply committed to that issue and has done a fairly significant job of improving that education. I don't think it's hit the ground level in every jurisdiction of every riding of every member yet, I agree with that.

● (1715)

Mr. David Tilson: Do you have a comment, Mr. Bowman?

Mr. Brian Bowman: Sure. I would echo the comments that have already been made in terms of the Privacy Commissioner's office and their staff doing a great job in public education. You're right in recognizing the reality that a lot of small and medium-sized businesses either don't care or don't understand the legislation. We don't think that radically overhauling the legislation is the answer to combat that, nor do we think that leaving it as confusing and subjective as some of the terms are is the answer.

The reality I face in my day-to-day practice is that small and medium-sized businesses are overwhelmed by the legislation. They don't understand it, and it's confusing, so they tune out and don't comply. Then they look at the Privacy Commissioner's office and they don't see order-making power, or they don't see the types of enforcement we've specifically addressed here, and again they tune out. That should be a real concern to everyone, including the organizations that have spent a lot of resources trying to comply with the legislation. The changes we've suggested we think are modest and would assist with small and medium-sized businesses. That's why some of the provisions that have influenced our submissions stem from the Alberta and British Columbia acts, which do a much better job of spoon-feeding to small and medium-sized businesses what they actually need to do to comply.

The Chair: Thank you, Mr. Tilson.

Mr. Van Kesteren, there's time, if you have a follow-up.

Mr. Dave Van Kesteren: We wanted a discussion. I appreciate, Professor, what you have brought to the table, that right for privacy. I'm just a little bit concerned about our own responsibilities.

You talked about this guy in the States who was so shocked to find out they could find out what movies you watch. Isn't there a responsibility for a process? At one time I had to worry about things like that or get in trouble with my wife, and now I've got to worry about my constituents. Isn't there some responsibility on our part?

Mr. Ian Kerr: I've never denied there's any responsibility with respect to agreeing or assenting to terms in a contract. That's never been my position. Interestingly, the courts in Canada took your position on this in another case we haven't talked about yet, a case called Kanitz v. Rogers Cable Inc. It had to do with Rogers wanting to change some of the terms of its agreement after the contract had already been made with its particular customers. The question was whether or not it could do so after the fact and have that still be part of the contract. Part of what the decision ultimately said was it was up to individuals to go and check Rogers' website to be able to know about the updated terms, and if they agreed to them and whatnot.

If you were to assign your legislative assistant or whoever helps you to be the babysitter of every standard form contract you've entered into this month alone, you wouldn't get a lot of help on any other things if you had to adopt that kind of approach across the board, given how automated these things are. Also, as you said previously, you didn't even know you signed that one.

The responsibility flows both ways. While you're right to point out that the consumer has responsibility in these matters, at the end of the day, if these automated contracts work in the direction of the one party who gets the opportunity to write them, that will be just as harmful to the small guy, whether it's a small business or an irresponsible consumer, in your view.

The Chair: Ms. Siegel, would you like the last word on this?

Mrs. Ariane Siegel: Yes, thank you.

I'm glad Professor Kerr raised that point, because this takes us back to the constitutional question. PIPEDA, the regulation of personal information in society, does not occur in a vacuum. For example, with respect to the case of notification of important changes in the contract, Ontario's brand new Consumer Protection Act deals with exactly that. It deals with requirements to provide explicit notification to consumers, if you ever want to change the terms of their contract on 30 days' notice. So we're moving into a realm where the provinces have a very important say in exactly how terms of contracts between private organizations and individuals are played out. PIPEDA is general because it has to leave some room for constitutional maneuverability in terms of what the provinces can legislate and what the federal government can legislate. Many of our consumer protections acts deal with that exact point.

● (1720)

The Chair: Thank you very much.

Colleagues, do you have any other questions?

Very briefly, Mr. Peterson.

Hon. Jim Peterson: If it works, don't fix it. But, Mr. Bowman, in terms of the order-making power, do you know of any horror stories that could have been avoided if the commissioner did have order-making power?

Mr. Brian Bowman: Any horror stories that would have occurred if the commissioner did have—

The Chair: Any horror stories that could have been avoided.

Mr. Brian Bowman: That could have been avoided if the commissioner had order-making power? I can't think of any off the top of my head. That's why we didn't recommend that the commissioner get order-making power.

Hon. Jim Peterson: Professor Kerr.

Mr. Ian Kerr: Yes. I would only be speculating, but it would be an interesting speculation to ask the question, how might an office, not necessarily that commissioner but an office, with order-making power have dealt with the situation where *Maclean's* magazine came and dumped all of the commissioner's cellphone records onto her desk, which she bought from a U.S. data broker? I think it would be an interesting question to ask.

Hon. Jim Peterson: Okay.

The Chair: I only have one question. Did you say, Professor Kerr, that people are blogging what's going on in this committee?

Mr. Ian Kerr: Yes, all the time.

The Chair: My goodness. Unbelievable!

I'd like to thank our witnesses. This is always interesting information. We appreciate the recommendations that were given and the answers that were given. We thank our witnesses for coming and for your expertise. We appreciate it.

Committee members, we still have a few minutes to deal with some business. Now we're on the third report of the steering committee, which has in fact been superceded to a degree by intervening events.

That reminds me, I want to remind committee members that we will have a special meeting tomorrow morning. It will start at 9:30 a.m., not at 9 a.m., so please don't be here at 9 a.m. The sole purpose of the meeting will be to interview Robert Marleau, who has been put forward as the new Information Commissioner of Canada.

Everybody has before them the third report. You can effectively ignore paragraph 1 because of what I've just said.

Now we're going to paragraph 2. You can effectively ignore nothing there. We'll talk about paragraph 2, then. Obviously we'll have one extra meeting available to us, because we won't need January 30 to interview Mr. Marleau.

Madame Lavallée.

[*Translation*]

Mrs. Carole Lavallée: I would like to verify whether it is possible to add a third sub-paragraph to reserve time on December 15, in case the Minister of Justice comes to introduce his strengthened and modernized access to information legislation.

That is what I am proposing.

[*English*]

The Chair: That issue was not dealt with; you got a chance to say it again. As always, we're in the hands of the committee. Right now we're talking about paragraph 2. Is there any discussion about paragraph 2? You'll notice that there are some timelines set out there.

I'm simply asking. If there is no discussion, I'll ask someone to move paragraph 2.

Hon. Jim Peterson: When do we come back?

The Chair: We come back in the last week in January. Our committee meetings, I'm told, have been changed, or will be changed. We will no longer be meeting on Monday and Wednesday; we'll be meeting on Tuesday and Thursday, 9 a.m. to 11 a.m. Our first meeting then would be January 30, Tuesday.

Hon. Jim Peterson: That's only six more meetings for hearings.

The Chair: Yes.

Mr. David Tilson: Mr. Chairman, on that, do I assume from what you're saying that it's because of paragraph 1 that there would be another meeting?

The Chair: That's correct.

Mr. David Tilson: So our first day back we would have—

The Chair: Yes, it will be Tuesday, January 30, and we'll get right into PIPEDA.

Mr. David Tilson: So there's an extra day there.

Hon. Jim Peterson: It's five more days for hearings.

I'd like to hear from you, Mr. Chair, and maybe the clerk, as to how many more witnesses want to appear before us.

The Chair: The steering committee, Mr. Peterson, went through the list of witnesses, and it was the judgment of the steering committee unanimously that this number of days would be able to adequately address the number of witnesses who requested an appearance and the issues they would be dealing with.

Hon. Jim Peterson: And I take it we will be having the Privacy Commissioner back for a final meeting for a full two hours?

The Chair: Yes, and we also want to have the Minister of Industry. You will recall that the bureaucracy said they would need the minister's instructions to provide us with their advice as to what they thought were or were not appropriate suggestions. So we'll have a meeting with the minister and we'll have a meeting with the Privacy Commissioner.

● (1725)

Hon. Jim Peterson: How many meetings are left with witnesses?

The Chair: Two.

Hon. Jim Peterson: Out of the six meetings? We've got one for Mr. Marleau, then we've got one for the Privacy Commissioner, then one for the minister—

The Chair: Forget Mr. Marleau because we're having an additional one. We have one Wednesday, we have two during the last week in January, so that's three, we have two in the first week in February, so that's five, and we have two more in the next week, so that's seven. And that should finish it. Of the seven, two will be for the Privacy Commissioner and the minister. So there are five meetings, and we would leave—

Hon. Jim Peterson: For witnesses.

The Chair: Nothing is written in stone. We believe we'll be able to conclude. If not, we'll come back and make a further recommendation.

Are there any other questions or comments?

Who'd like to move paragraph 2?

Mr. Mike Wallace: I'll move it.

The Chair: Mr. Wallace will move it.

We need an amendment? What kind of amendment would you like? We will add January 30 to paragraph 2 or what?

The Clerk of the Committee (Mr. Richard Rumas): That Robert Marleau will appear tomorrow.

The Chair: All right.

That the committee invite Robert Marleau to a meeting scheduled for December 12, 2006.

Mr. Mike Wallace: Moved as amended.

The Chair: All in favour? Opposed, if any?

(Motion as amended agreed to)

The Chair: We have two minutes.

Madam Lavallée, do you have a motion that you wish to discuss in two minutes?

Mr. Mike Wallace: Madam Lavallée said Wednesday, and I think we should leave it until Wednesday's meeting.

[*Translation*]

Mrs. Carole Lavallée: No, let's talk about it now. There are only four days before December 15, as you know, Mr. Chair.

We passed with majority a motion calling on the Minister of Justice to introduce in the House of Commons strengthened and modernized access to information legislation no later than December 15.

I think it would be a good idea to give the minister a friendly reminder. We could ask him for a status report and when, by December 15, he plans to introduce the bill. Since the motion asked him to introduce it no later than December 15, he could introduce it tomorrow in the House.

I am asking that we pass this motion in order to be able to communicate with him as soon as possible so that he can tell us when, by Friday, he will introduce the bill.

Thank you, Mr. Chair.

[*English*]

The Chair: Mr. Peterson.

Hon. Jim Peterson: Her idea would be to have a meeting and he could deposit the new bill right here on the 15th.

Some hon. members: It's good idea.

The Chair: Is there any other discussion?

[*Translation*]

Mrs. Carole Lavallée: That would be perfect, but not the 15th because we will not be here, Mr. Peterson.

[*English*]

The Chair: Mr. Dhaliwal.

Mr. Sukh Dhaliwal: Mr. Chair, if Madam Lavallée is going to bring in the motion, I think we should have it as the very first thing on the next meeting.

The Chair: Mr. Dhaliwal, we have invited—and the committee has agreed to this—these witnesses, and in courtesy to them we'll put the motion as item number two, after we have heard from our witnesses. Otherwise we may end up filibustering, possibly—I'm not suggesting that—and end up having our witnesses, who may have come from some distance, sitting there listening to a discussion for two hours. I think it's more productive if we have our witnesses first, and then if there's time remaining, we'll discuss the motion of Madam Lavallée.

Mr. Wallace.

Mr. Mike Wallace: I'm somewhat unclear. And I'm not trying to fill in time. I don't mind going to a vote. If this gets passed today.... I think she's putting it forward. Am I not correct?

The Chair: Yes, that's correct.

Mr. Mike Wallace: Then we will still hear our witnesses before we get the minister back here to deal with this particular item?

The Chair: No. The motion is simply for the chair to write to the minister and ask for a progress report on what's happened.

Mr. Mike Wallace: So it's just writing a letter.

The Chair: It's just writing a letter.

Mr. Mike Wallace: Why didn't you say that last week?

The Chair: It's just writing a letter. That's the answer. We will still hear from our witnesses.

I see 5:30 has come.

The meeting is adjourned.

Published under the authority of the Speaker of the House of Commons

Publié en conformité de l'autorité du Président de la Chambre des communes

Also available on the Parliament of Canada Web Site at the following address:
Aussi disponible sur le site Web du Parlement du Canada à l'adresse suivante :
http://www.parl.gc.ca
